WE CLAIM:

1. A method for verifying integrity of a computing process, comprising:

determining a trait associated with the computing process;

determining a pattern statistic associated with the trait based in part on an execution of the computing process in a normal condition;

determining a prototype statistic associated with the trait based in part on another execution of the computing process in another condition;

comparing the pattern statistic to the prototype statistic; and

if the comparison indicates abnormal behavior the computing process, performing a predetermined action.

2. The method of claim 1, wherein performing the predetermined action further comprises performing at least one of sending an alert message, and disabling the computing process.

3. The method of claim 1, wherein the trait further comprises at least one system level call.

4. The method of claim 1, wherein determining the pattern statistic and the prototype statistic further comprises:

determining a trend associated with the trait during execution of the computing process in the normal condition; and

determining another trend associated with the trait during the other execution of the computing process in the other condition.

5. The method of claim 1, wherein comparing the pattern statistic to the prototype statistic further comprises comparing a frequency and a consequence associated with the pattern statistic to another frequency and another consequence associated with the prototype statistic.

6. The method of claim 1, wherein determining the pattern statistic further comprises:

determining consecutive data associated with the trait;

employing a graphical representation to convert the consecutive data to a radius-vector;

if the radius-vector is mature, retaining an endpoint coordinate associated with the radius-vector;

determining a frequency pattern associated with the trait; and

employing the graphical representation in part to convert the frequency pattern to an average directional vector.

7. The method of claim 6, wherein the mature radius-vector further comprises satisfying a condition wherein an absolute difference between a first sequence error and a second sequence error is less than or equal to a predetermined value.

8. The method of claim 6, wherein employing the graphical representation further comprises employing a chaos game representation (CGR) plot.

9. The method of claim 1, wherein comparing the pattern statistic to the prototype statistic further comprises comparing a vector norm and angle to another vector norm and another angle.

10. The method of claim 1, wherein comparing the pattern statistic to the prototype statistic further comprises:

determining a pattern vector associated with the pattern statistic, wherein the pattern vector includes a direction and length;

determining a prototype vector associated with the prototype statistic, wherein the prototype vector includes another direction and another length;

determining a total difference between the pattern vector and the prototype vector; and

if the total difference is outside a predetermined confidence level, indicating that the prototype statistic is associated with abnormal behavior.

11. An apparatus encoded with computer-executable components for determining tamper evidence of a client process, comprising:

a transceiver arranged to receive and forward data;

an interface, coupled to the transceiver, and arranged to perform actions, including:

determining a trait associated with the client process;

receiving a first set of data associated with the trait based in part on execution of the client process in a normal condition;

receiving a second set of data associated with the trait based in part on another execution of the client process in another condition;

determining a pattern statistic associated with the first set of data;

determining a prototype statistic associated with the second set of data;

comparing the pattern statistic to the prototype statistic; and

if the comparison indicates abnormal behavior of the client process, performing a predetermined action.

12. The apparatus of claim 11, wherein the computer-executable components reside in at least one of a server, and a client.

13. The apparatus of claim 11, wherein performing the predetermined action further comprises performing at least one of sending an alert message, and disabling the computing process.

14. The apparatus of claim 11, wherein the trait further comprises at least one system level call.

15. The apparatus of claim 11, wherein determining the pattern statistic and the prototype statistic further comprises:

determining a trend associated with the trait during execution of the client process in the normal condition; and

determining another trend associated with the trait during the other execution of the client process in the other condition.

16. The apparatus of claim 11, wherein determining the pattern statistic further comprises:

determining consecutive data associated with the trait;

employing a graphical representation to convert the consecutive data to a radius-vector;

if the radius-vector is mature, retaining an endpoint coordinate associated with the radius-vector;

determining a frequency pattern associated with the trait; and

employing the graphical representation to convert the frequency pattern to an average directional vector.

17. The apparatus of claim 16, wherein the mature radius-vector further comprises satisfying a condition wherein an absolute difference between a first sequence error and a second sequence error is less than or equal to a predetermined value.

18. The apparatus of claim 16, wherein employing the graphical representation further comprises a chaos game representation (CGR) plot.

19. The apparatus of claim 11, wherein comparing the pattern statistic to the prototype statistic further comprises:

determining a pattern vector associated with the pattern statistic;

determining a prototype vector associated with the prototype statistic;

determining a total difference between the pattern vector and the prototype vector; and

if the total difference is outside a predetermined confidence level, indicating that the prototype statistic is associated with abnormal behavior.

20. A system for determining tamper evidence of a computing process, comprising:

a client that includes the computing process, and is configured to communicate trait data associated with an execution of the computing process; and

a server, coupled to the client, and arranged to perform actions, including:

receiving a first set of data associated with the trait based in part on execution of the computing process in a normal condition;

receiving a second set of data associated with the trait based in part on another execution of the computing process in another condition;

determining a pattern statistic associated with the first set of data;

determining a prototype statistic associated with the second set of data;

comparing the pattern statistic to the prototype statistic; and

if the comparison indicates abnormal behavior of the computing process, performing a predetermined action.

21. The system of claim 20, wherein comparing the pattern statistic to the prototype static further comprises employing a graphical representation to compare the pattern statistic to the prototype statistic.

22. An apparatus for verifying integrity of a computing process, comprising:

a means for determining a trait associated with the computing process;

a means for determining a pattern statistic associated with the trait based in part on execution of the computing process in a normal condition;

a means for determining a prototype statistic associated with the trait based in part on another execution of the computing process in another condition;

a means for comparing the pattern statistic to the prototype statistic, and

if the comparison indicates abnormal behavior, a means for performing a predetermined action